



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/057,255	01/24/2002	Masashi Hamada	1232-4812	2744
27123 7590 02/15/2007 MORGAN & FINNEGAN, L.L.P. 3 WORLD FINANCIAL CENTER NEW YORK, NY 10281-2101			EXAMINER SERRAO, RANODHI N	
			ART UNIT 2141	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	DELIVERY MODE
3 MONTHS			02/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

**Office Action Summary**

Application No.

10/057,255

Applicant(s)

HAMADA, MASASHI

Examiner

Ranodhi Serrao

Art Unit

2141

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 28 December 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1,4-10,12-15,17-19,22-24,26-35,38,61 and 84 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,4-10,12-15,17-19,22-24,26-35,38,61 and 84 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### ***Response to Arguments***

1. Applicant's arguments with respect to claims 1, 4-10, 12-15, 17-19, 22-24, 26-35, 38, 61, and 84 have been considered but are moot in view of the new ground(s) of rejection.
2. The applicant argued in substance the newly added limitations of claims 1, 4, and 12-14. However, the new grounds teach these and the added features. See rejections below.

### ***Claim Rejections - 35 USC § 103***

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
4. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Petersen (2002/0103907) and Staheli et al. (5,537,533).
5. As per claim 1, Petersen teaches a data management method using a network system which includes a server, a client terminal and a plurality of data servers (see Petersen, ¶ 60), comprising: a reception step of making the server receive a user's data storage request and data to be stored from the client terminal; a select step of making the server automatically select data servers for storing the data from the plurality of data servers (see Petersen, ¶ 67), the selected data servers being different from each other and including at least a first data server and a second data server (see Petersen, ¶ 60), said first data server being located in an area which is different from an area of user's

Art Unit: 2141

address registered by the user of the client terminal (see Petersen, ¶ 17); and a storage step of making the server send the data to the selected data servers, and store the data in the selected data servers (see Petersen, ¶ 69). But fails to teach said second data server being located in an area with a disaster rate of occurrence equal to or smaller than a predetermined threshold. However, Staheli et al. teaches said second data server being located in an area with a disaster rate of occurrence equal to or smaller than a predetermined threshold (see Staheli et al., col. 1, lines 47-56 and col. 14, lines 54-62: wherein the limitation, "a disaster rate of occurrence equal to or smaller than a predetermined threshold" can be interpreted broadly to mean a server that is a safe distance away from the client. This is disclosed by Staheli et al.). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Petersen to said second data server being located in an area with a disaster rate of occurrence equal to or smaller than a predetermined threshold in order to protect mission-critical data in a client-server computer network as part of a business recovery plan, and to remotely mirror data such that a substantially concurrent copy of the critical data stored on a primary network server is also continuously available on a replacement network server which is located at a safe distance from the primary network server (see Staheli et al., col. 1, lines 8-15).

6. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Petersen and Staheli et al. as applied to claim 1 above, and further in view of Day et al. (2002/0095487) and Satomi et al. (6,347,384). Petersen and Staheli et al. teach the

Art Unit: 2141

mentioned limitations of claim 1 above and furthermore Staheli et al. teaches a disaster rate of occurrence equal to or smaller than a predetermined threshold (see Staheli et al., col. 1, lines 47-56 and col. 14, lines 54-62) but fail to teach a method further comprising: a step of making the server acquire disaster information from a disaster information database that provides disaster information, and search for the area with a disaster rate of occurrence on the basis of the acquired disaster information for selecting the server in the select step. However, Satomi et al. teaches a method further comprising: a step of making the server acquire disaster information from a disaster information database that provides disaster information (see Satomi et al., column 2, lines 28-50). And Day et al. teaches search for a server for selecting the server in the select step (see Day et al., ¶ 54). It would have been obvious to one having ordinary skill in the art at the time of the invention to combine searching for a server with searching for the area with a disaster rate of occurrence on the basis of the acquired disaster information since Day et al. teaches searching for a server and Shannon teaches a data server located in an area with a disaster rate of occurrence.

Furthermore, it would have been obvious to one having ordinary skill in the art at the time of the invention to modify Petersen and Staheli et al. to a method further comprising: a step of making the server acquire disaster information from a disaster information database that provides disaster information, and search for the area with a disaster rate of occurrence on the basis of the acquired disaster information for selecting the server in the select step in order to provide a system that is capable of

rapidly and effectively making and carrying out a plan for dealing with a disaster when it occurs (see Satomi et al., col. 1, lines 45-48).

7. Claims 7 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Petersen and Staheli et al. as applied to claim 1 above, and further in view of and Satomi et al.

8. As per claims 7 and 9, the above-mentioned motivation of claim 4 applies fully in order to combine Petersen, Staheli et al., and Satomi et al.

9. As per claim 7, Petersen, Staheli et al., and Satomi et al. teach a method further comprising: a step of making the server send to the client terminal addresses of the data servers that store the data (see Satomi et al., column 2, lines 51-62).

10. As per claim 9, Petersen, Staheli et al., and Satomi et al. teach a method wherein information of the user's address is pre-stored in the server (see Satomi et al., column 2, lines 51-62 and column 5, lines 14-39).

11. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Petersen and Staheli et al. as applied to claim 1 above, and further in view of Beeler, Jr. (5,189,020).

12. As per claim 5, Petersen and Staheli et al. teach the mentioned limitations of claim 1 above but fail to teach a method further comprising: a step of making the server encrypt the data, and wherein the storage step includes the step of: making the server send the data encrypted by different methods to the respective data servers, and store the data in the data servers. However, Beeler, Jr. teaches a method further comprising:

Art Unit: 2141

a step of making the server encrypt the data, and wherein the storage step includes the step of: making the server send the data encrypted by different methods to the respective data servers, and store the data in the data servers (see Beeler, Jr., column 17, lines 10-21). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Petersen and Staheli et al. to a method further comprising: a step of making the server encrypt the data, and wherein the storage step includes the step of: making the server send the data encrypted by different methods to the respective data servers, and store the data in the data servers in order to prevent replicated data from being intercepted and compromised (see Beeler, Jr., col. 7, lines 34-41).

13. As per claim 6, the above-mentioned motivation of claim 5 applies fully in order to combine Petersen, Staheli et al., and Beeler, Jr.

14. As per claim 6, Beeler, Jr., Petersen, and Staheli et al. teach the step of making the server periodically acquire the encrypted data from the data servers (see Beeler, Jr., column 17, lines 10-21); the step of making the server decrypt the acquired data; and the step of making the server compare the decrypted data (see Beeler, Jr., column 18, lines 7-19).

15. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Petersen, Staheli et al., and Beeler, Jr. as applied to claims 1 and 5 above, and further in view of Satomi et al. and Bowman-Amuah (6,289,382). Petersen, Staheli et al., and Beeler Jr. teaches the mentioned limitations of the above claims but fails to teach a step

Art Unit: 2141

of making the server send to the client terminal addresses of the data servers that store the data, and a key used to decrypt the encrypted data. Satomi et al. teaches the step of making the server send to the client terminal addresses of the data servers that store the data (see Satomi et al., column 2, lines 51-62). And Bowman-Amuah teaches a key used to decrypt the encrypted data (Bowman-Amuah, column 79, lines 39-41). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add the step of making the server send to the client terminal addresses of the data servers that store the data in order to meet the predefined priority of communication networks over which to reach a desired server. And a key used to decrypt the encrypted data in order to prevent unauthorized interception of data.

16. Claims 15, 17-19, 23-28, and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beeler, Jr., Petersen, Staheli et al., and Byrd et al. (6,069,941).

17. As per claims 15, Petersen and Staheli et al. teach the mentioned limitations of claim 12 above, but fail to teach a server, wherein said select means automatically selects the data server based on the user's service subscription qualification level. However, Byrd et al. teaches a server, wherein said select means automatically selects the data server based on the user's service subscription qualification level (see Byrd et al., col. 5, lines 26-52). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Petersen and Staheli et al. to a server, wherein said select means automatically selects the data server based on the user's service subscription qualification level in order to connect a qualified subscriber to services



Art Unit: 2141

while monitoring the amount of service being supplied (see Byrd et al., col. 2, lines 19-35).

18. As per claim 17, Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12 and 15 above but fail to teach wherein said sending means encrypts the data using an encryption method corresponding to the data servers selected by said select means. Beeler, Jr. however teaches wherein said sending means encrypts the data using an encryption method corresponding to the data servers selected by said select means (see Beeler, Jr., column 17, lines 10-21). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add wherein said sending means encrypts the data using an encryption method corresponding to the data servers selected by said select means in order to prevent replicated data from being intercepted and compromised.

19. As per claim 18, Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12 and 15 above but Beeler, Jr., Petersen, and Staheli et al. fail to teach wherein the service subscription qualification level is determined based on a subscription fee for a service. Byrd et al. however teaches wherein the service subscription qualification level is determined based on a subscription fee for a service (see Byrd et al., column 2, lines 59-65). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add wherein the service subscription qualification level is determined based on a subscription fee for a service in order to monitor the amount of service being supplied to a subscriber.

20. As per claim 19, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12 and 15 above but Beeler, Jr., Petersen, and Staheli et al. fail to teach wherein the service subscription qualification level is determined based on a service subscription term. Byrd et al. however teaches the service subscription qualification level is determined based on a service subscription term (see Byrd et al., column 2, lines 59-65). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add the service subscription qualification level is determined based on a service subscription term in order to monitor the amount of service being supplied to a subscriber.

21. As per claim 23, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12 and 15 above but Beeler, Jr., Petersen, and Staheli et al. fail to teach wherein when the user's service subscription qualification level has changed, said select means re-selects the data servers, and said sending means sends the data again to the at least one data server re-selected by said select means. Byrd et al. however teaches wherein when the user's service subscription qualification level has changed, said select means re-selects the data server, (see Byrd et al., column 4, lines 27-48), and said sending means sends the data again to the data servers re-selected by said select means (see Byrd et al., column 4, lines 49-58). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add wherein when the user's service subscription qualification level has changed, said select means re-selects the servers, and said sending means sends the

Art Unit: 2141

data again to the data servers re-selected by said select means in order to qualify the subscriber in accordance with the subscriber's telephone number.

22. As per claim 24, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12 and 15 above but Beeler, Jr., Petersen, and Staheli et al. fail to teach wherein said select means re-selects the data servers in accordance with a change in disaster information, and said sending means sends the data request again to the data servers re-selected by said select means. Byrd et al. however teaches wherein said select means re-selects the data servers in accordance with a change in disaster information, (see Byrd et al., column 4, lines 27-48), and said sending means sends the data again to the data servers re-selected by said select means (see Byrd et al., column 4, lines 49-58). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add wherein said select means re-selects the data servers in accordance with a change in disaster information, and said sending means sends the data again to the data servers re-selected by said select means in order to qualify the subscriber in accordance with the subscriber's telephone number.

23. As per claim 26, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12 and 15 above but Byrd et al., Petersen, and Staheli et al. fail to teach checking means for checking authenticity of the data stored in the data server. Beeler, Jr. however teaches checking means for checking authenticity of the data stored in the data server (see Beeler, Jr., column 17, lines 9-21: wherein compression and encryption serves the function of authenticity). It would have been

Art Unit: 2141

obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add checking means for checking authenticity of the data stored in the data server in order to prevent replicated data from being intercepted and compromised.

24. As per claim 27, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12, 15 and 26 above but Byrd et al., Petersen, and Staheli et al. fail to teach wherein said checking means checks authenticity by comparing data which are associated with an identical storage request and are stored in the data servers. Beeler, Jr. however teaches wherein said checking means checks authenticity by comparing data which are associated with an identical storage request and are stored in the data servers (see Beeler, Jr., column 18, lines 7-19). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add wherein said checking means checks authenticity by comparing data which are associated with an identical storage request and are stored in the data servers in order to prevent replicated data from being intercepted and compromised.

25. As per claim 28, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12, 15, and 26 above but Petersen, Staheli et al., and Byrd et al. fail to teach wherein said checking means checks if data becomes fraudulent due to a memory medium. Beeler, Jr. however teaches wherein said checking means checks if data becomes fraudulent due to a memory medium (see Beeler, Jr., column 7, lines 34-41: wherein replication data is transmitted through a memory medium). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add wherein said checking means checks if data becomes

fraudulent due to a memory medium in order to prevent replicated data from being intercepted and compromised.

26. As per claim 33, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12 and 15 above but Petersen, Staheli et al., and Byrd et al. fail to teach notify means for sending at least various storage condition data associated with a data storage process to a client terminal that issued the storage request. Beeler, Jr. however teaches notify means for sending at least various storage condition data associated with a data storage process to a client terminal that issued the storage request (see Beeler, Jr., column 10, lines 20-31: wherein broadcasting a message serves the function of notify means). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add notify means for sending at least various storage condition data associated with a data storage process to a client terminal that issued the storage request in order to determine if the node is configured as a target server.

27. As per claim 34, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12, 15 and 33 above but Petersen, Staheli et al., and Byrd et al. fail to teach wherein said notify means sends encryption algorithm and key data in addition to storage location data of the data associated with the storage request as the storage condition data. Beeler, Jr. however teaches wherein said notify means sends encryption algorithm and key data in addition to storage location data of the data associated with the storage request as the storage condition data (see Beeler, Jr., column 17, lines 9-21). It would have been obvious to one having ordinary skill in the art

Art Unit: 2141

at the time of the invention to modify the above claim to add wherein said notify means sends encryption algorithm and key data in addition to storage location data of the data associated with the storage request as the storage condition data in order to replicate the operation described in each packet to the local storage media on target server and restore data to source server when necessary.

28. As per claim 35, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12, 15, and 33 above but Byrd et al., Petersen, and Staheli et al. fail to teach wherein the client device includes storage means for storing at least the storage condition data sent from said notify means. Beeler, Jr. however teaches wherein the client device includes storage means for storing at least the storage condition data sent from said notify means (see Beeler, Jr., column 10, line 65-column 11, line 10). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add wherein the client device includes storage means for storing at least the storage condition data sent from said notify means in order to replicate the operation described in each packet to the local storage media on target server and restore data to source server when necessary.

29. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Beeler, Jr., Petersen, Staheli et al., Byrd et al., and Weinman, Jr. (2001/0047412). Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12 and 15 above and furthermore Byrd et al. teaches servers corresponding to the service subscription qualification level of the user who issued the storage request (see Byrd et

al., col. 5, lines 26-52). But Beeler, Jr., Byrd et al., Petersen, and Staheli et al. fail to teach wherein said select means selects a data server with a lowest suffering risk from the plurality of data servers and a server with a lowest suffering risk of the data servers in a different area from the area of user's address registered by the user who issued the storage request. However Weinman, Jr. teaches wherein said select means selects a data server with a lowest suffering risk from the plurality of data servers (see Weinman, Jr., ¶ 24) and a server with a lowest suffering risk of the data servers in a different area from the area of user's address registered by the user who issued the storage request (see Weinman, Jr., ¶ 43). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Beeler, Jr., Petersen, and Staheli et al., and Byrd et al. to wherein said select means selects a data server with a lowest suffering risk from the plurality of data servers and a server with a lowest suffering risk of the data servers in a different area from the area of user's address registered by the user who issued the storage request in order to mirror and relay computer data to improve continuity of data by maximizing the distance between two copies of the data in synchronous mode, zero data loss environments (see Weinman, Jr., abstract).

30. Claims 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beeler, Jr., Petersen, Staheli et al., and Byrd et al. as applied to claims 12, 15, and 26 above, and further in view of Bowman-Amuah (6,289,382).

31. As per claim 29, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12, 15, and 26 above but fail to teach wherein said

Art Unit: 2141

checking means checks if data becomes fraudulent due to tampering of data. Bowman-Amuah however teaches wherein said checking means checks if data becomes fraudulent due to tampering of data (column 128, line 62-column 129, line 10). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add wherein said checking means checks if data becomes fraudulent due to tampering of data in order to fulfill distinct business services through well-defined interfaces.

32. As per claim 30, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12, 15, 26, and 29 above but fail to teach wherein when said checking means determines that the data becomes fraudulent due to tampering of data, said checking means sends a message indicating this to a client terminal that issued the storage request of the data. Bowman-Amuah however teaches wherein when said checking means determines that the data becomes fraudulent due to tampering of data, said checking means sends a message indicating this to a client terminal that issued the storage request of the data (column 128, line 62-column 129, line 10). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add wherein when said checking means determines that the data becomes fraudulent due to tampering of data, said checking means sends a message indicating this to a client terminal that issued the storage request of the data in order to fulfill distinct business services through well-defined interfaces.



Art Unit: 2141

33. As per claim 31, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims 12 and 15 above but fail to teach authentication means for authenticating if the user who issued the storage request is a member who subscribes to the service, and accepts only the storage request from the user authenticated by said authentication means. Bowman-Amuah however teaches authentication means for authenticating if the user who issued the storage request is a member who subscribes to the service, and accepts only the storage request from the user authenticated by said authentication means (column 79, lines 4-13). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add authentication means for authenticating if the user who issued the storage request is a member who subscribes to the service, and accepts only the storage request from the user authenticated by said authentication means in order to prevent unauthorized interception of data.

34. As per claim 32, Beeler, Jr., Petersen, Staheli et al., and Byrd et al. teach the mentioned limitations of claims, 12 and 15 above but fail to teach authentication means for checking authenticity of the data server selected by said select means, and said sending means sends data in only the data servers authenticated by said authentication means. Bowman-Amuah however teaches authentication means for checking authenticity of the data server selected by said select means, and said sending means sends data in only the data servers authenticated by said authentication means (column 81, lines 47-67). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the above claim to add authentication means for

Art Unit: 2141

checking authenticity of the data server selected by said select means, and said sending means sends data in only the data servers authenticated by said authentication means in order to verify network access requests by validating that users are who they claim to be.

35. Claims 10 and 12-14, 38, 61, and 84 have similar limitations as to claims 1, 4-9, 15, 17-19, 22-24, 26-35 above; therefore, they are being rejected under the same rationale.

### ***Conclusion***


**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ranodhi Serrao whose telephone number is (571)272-7967. The examiner can normally be reached on 8:00-4:30pm, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571)272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
RUPAL DHARIA  
SUPERVISORY PATENT EXAMINER